IFW

Serial No.: 10/761,512

PATENT
PF030028

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Philippe Leyendecker; Jean-Maurice Cueff; Daniel Creusot
Serial No.	:	10/761,512
Filed	:	January 20, 2004
For	:	SYSTEM FOR RECEIVING BROADCAST DIGITAL DATA COMPRISING A MASTER DIGITAL TERMINAL, AND AT LEAST ONE SLAVE DIGITAL TERMINAL

PRIORITY DOCUMENT UNDER 35 U.S.C. 119

Commissioner for Patent
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Attached hereto are certified copies of the priority documents referred to in the Declaration, the priorities of which are claimed in the Declaration. The priority documents are as follows:

French 03/00941 filed January 20, 2003

European 03291099.4 filed May 7, 2003

Respectfully submitted,

Philippe Leyendecker
Jean-Maurice Cueff
Daniel Creusot

By: _____
Kuniyuki Akiyama
Registration No.: 43,314
(609) 734-6801

THOMSON Licensing Inc.
Patent Operations
PO Box 5312
Princeton, NJ 08543-5312

Date: June 22, 2004

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in a postage paid envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date indicated below.

Date: June 22, 2004 Signature Wanda Tornabene

1°761512

CERTIFIED COPY OF PRIORITY DOCUMENT

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 19 DEC. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

REQUÊTE EN DÉLIVRANCE page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ W / 210502

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 20 JAN. 2003
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0300941
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 20-01-03

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

THOMSON
Karine BERTHIER
46 Quai Alphonse Le Gallo
92648 Boulogne cedex
FRANCE

Vos références pour ce dossier *(facultatif)* PF030028

Confirmation d'un dépôt par télécopie ☒ N° attribué par l'INPI à la télécopie 2157

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Système de réception de données numériques diffusées comprenant un terminal numérique maître, et au moins un terminal numérique esclave

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date N°
	Pays ou organisation Date N°
	Pays ou organisation Date N°
	☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR (Cochez l'une des 2 cases)		☒ Personne morale ☐ Personne physique
Nom ou dénomination sociale		THOMSON LICENSING S.A.
Prénoms		
Forme juridique		S.A.
N° SIREN		3 8 3 4 6 1 9 1
Code APE-NAF		3 2 2 A
Domicile ou siège	Rue	46 Quai Alphonse Le Gallo
	Code postal et ville	9 2 1 0 0 Boulogne Billancourt
	Pays	FRANCE
Nationalité		française
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		
		☐ S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

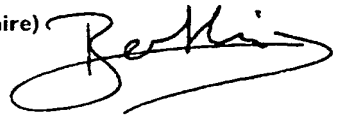
REMISE DES PIÈCES
DATE 20 JAN. 2003
LIEU CG

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0300941

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		BERTHIER
Prénom		Karine
Cabinet ou Société		THOMSON
N °de pouvoir permanent et/ou de lien contractuel		9016
Adresse	Rue	46 Quai Alphonse Le Gallo
	Code postal et ville	9 2 6 4 8 Boulogne cedex
	Pays	FRANCE
N° de téléphone *(facultatif)*		01 41 86 54 88
N° de télécopie *(facultatif)*		01 41 86 56 33
Adresse électronique *(facultatif)*		karine.berthier@thomson.net
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)*: **AG**
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
Karine Berthier
Mandataire



VISA DE LA PRÉFECTURE OU DE L'INPI

L. GUICHET

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention concerne un système de réception de données numériques diffusées comprenant un terminal numérique maître, et au moins un terminal numérique esclave raccordé au terminal maître.

Le marché des décodeurs de télévision numériques arrive actuellement à un tournant. La plupart des abonnés, dans les pays Européens notamment, sont équipés d'un seul terminal numérique (ou « décodeur ») par foyer alors qu'ils possèdent souvent au moins deux téléviseurs. Il existe donc une demande pour des équipements multiples en termes de décodeurs pour un même foyer.

Certains opérateurs de télévision numérique payante souhaitent offrir à leurs abonnés la possibilité de s'équiper de plusieurs terminaux numériques pour bénéficier de leurs services sur chacun des téléviseurs installés dans leur logement, sans pour autant leur faire payer pour les terminaux supplémentaires le prix d'un abonnement plein tarif, qui serait prohibitif, mais plutôt un tarif réduit (voire nul). Cependant il s'agit, pour l'opérateur, de s'assurer que les terminaux et abonnements « associés » restent effectivement dans le même foyer, car dans le cas contraire, ses revenus risquent d'en être considérablement affectés.

Une solution connue consiste à utiliser la « voie de retour » des terminaux numériques en demandant à l'abonné de relier tous les terminaux de son domicile à une même ligne téléphonique. L'opérateur contrôle ensuite périodiquement la connexion des terminaux à cette ligne téléphonique en télécommandant des appels téléphoniques des terminaux vers un serveur de l'opérateur. Cependant cette solution n'est pas satisfaisante car elle impose la connexion permanente des terminaux numériques de l'abonné à une ligne téléphonique.

Une autre solution décrite dans la demande de brevet français No 02 09362 déposée le 24 juillet 2002 par le même demandeur que la présente demande, THOMSON Licensing S.A., consiste à garantir qu'un lien de communication physique existe toujours entre un terminal secondaire (ou terminal « esclave ») et un terminal principal (ou terminal « maître ») avec lequel il est appairé. Le ou les terminaux esclaves (pour lequel ou lesquels l'abonné bénéficie d'un tarif préférentiel) ne peuvent fonctionner, c'est à dire fournir des données en clair au téléviseur auquel ils sont raccordés, sans vérification de la présence du terminal « maître » auquel ils sont appairés à proximité.

Plusieurs stratégies de communication entre ces décodeurs sont envisageables mais certaines peuvent présenter des risques de « piratage » ou de « contournement ».

Un but de la présente invention est d'apporter un perfectionnement à l'invention décrite dans la demande de brevet précitée en minimisant les risques de piratage ou de contournement

Le principe de l'invention est le suivant : Un terminal numérique « maître » contient une carte à puce dans laquelle sont enregistrés des droits payés par l'abonné au tarif normal. Un terminal numérique « esclave » contient une carte à puce dont les droits, identiques ou non à ceux de la carte à puce du décodeur « maître », ont été payés moins cher par le même abonné.

Ce tarif préférentiel de l'abonnement du décodeur « esclave » est accordé par l'opérateur avec l'accord tacite qu'il soit utilisé par le même abonné dans le même logement que le décodeur « maître ».

L'idée de base à l'origine de l'invention consiste à considérer que si le terminal numérique « esclave » n'est pas à proximité immédiate du terminal numérique « maître », il est utilisé dans un logement différent et donc l'abonné viole le contrat lui permettant de bénéficier d'un tarif préférentiel. Grâce à la présente invention, si une telle situation d'utilisation frauduleuse du terminal numérique « esclave » est détectée, ce dernier cesse de fonctionner normalement ; en l'occurrence, il ne permet plus à l'abonné d'accéder à l'ensemble des services qu'il est censé recevoir (image et son).

On notera que l'invention peut être mise en œuvre entre un terminal numérique maître et plusieurs esclaves, si l'opérateur le permet.

L'objet de l'invention est un système de réception de données numériques diffusées comprenant un terminal numérique maître, et au moins un terminal numérique esclave raccordé au terminal maître par une liaison et susceptible de recevoir des données numériques protégées. Selon l'invention, le terminal numérique esclave ne peut accéder aux données protégées que si des informations nécessaires pour accéder auxdites données et reçues par le terminal numérique maître sont transmises par l'intermédiaire de ladite liaison au terminal numérique esclave dans un délai prédéterminé.

Les données numériques protégées sont notamment des services de télévision embrouillées par des clés et les informations pour accéder aux données protégées sont notamment des messages contenant des droits d'accès aux services ou bien des paramètres permettant d'extraire de tels

messages des données reçues ou bien encore des messages contenant une partie des droits d'accès.

Selon une caractéristique particulière de l'invention, les informations reçues par le terminal numérique maître sont transformées avant d'être transmises au terminal numérique esclave. Notamment, les informations reçues par le terminal numérique maître sont reçues du système de diffusion sous une forme cryptée et sont décryptées dans le terminal maître avant d'être transmises au terminal esclave.

Pour résumé, le mécanisme de base de l'invention est le suivant :

- le terminal numérique maître reçoit une partie des éléments nécessaires au désembrouillage des services par le terminal numérique esclave ;

- ces éléments sont transmis au terminal numérique esclave dans des conditions bien définies et de manière unique par l'intermédiaire d'une liaison physique de communication entre les 2 terminaux ;

- si le terminal numérique maître n'est pas en mesure de fournir ces éléments au terminal numérique esclave dans un délai prédéterminé, le terminal numérique esclave n'est sera pas capable d'accéder au service reçu.

Les avantages de l'invention sont les suivants : comme elle se base sur des éléments de sécurité du système de diffusion lui-même (les informations échangées entre les terminaux sont cryptées avec des secrets gérés par le système de diffusion des données et par les cartes à puce des terminaux numériques), le risque de piratage au niveau de la carte à puce ou du terminal numérique est réduit.

D'autre part, comme l'invention s'appuie sur l'aspect « temps réel » de l'implémentation, ceci élimine le risque de prolongation de la liaison physique entre deux terminaux numériques par un réseau téléphonique ou Internet. En effet, la liaison physique entre les deux terminaux numériques maître et esclave pourrait être « rallongée » indéfiniment par une liaison Internet : l'opérateur de service n'aurait alors plus la garantie que les deux terminaux se trouvent dans le même foyer d'un abonné. En imposant, selon le principe de l'invention, un délai maximum pour le transfert des données, on s'assure ainsi que les informations ne transitent pas par une liaison de type Internet.

Un autre avantage de l'invention est qu'elle garantit que chaque échange de données est différent du précédent, et donc non-prédictible. En effet, un pirate pourrait être tenté d'espionner les informations qui sont reçues par les terminaux pour émuler les informations attendues de la part du terminal

numérique maître par le terminal numérique esclave à l'aide d'un dispositif pirate (un ordinateur par exemple). Comme les informations qui sont échangées entre les terminaux changent à chaque communication, elles sont non-prédictibles et ne peuvent donc être facilement émulées par un dispositif pirate.

L'invention sera mieux comprise à la lecture de la description détaillée qui va suivre de plusieurs modes de réalisation. Cette description est donnée uniquement à titre d'exemple et se réfère aux dessins annexés sur lesquels :

La figure 1 représente un schéma synoptique d'un système selon l'invention.

La figure 2 illustre un premier mode de réalisation de l'invention.

La figure 3 illustre un second mode de réalisation de l'invention.

La figure 4 illustre un troisième mode de réalisation de l'invention.

La figure 5 illustre une variante du second mode de réalisation.

La figure 6 illustre un quatrième mode de réalisation.

Sur la figure 1, nous avons représenté deux terminaux numériques (ou décodeurs) : un terminal maître 1 et un terminal esclave 2, qui sont reliés par une liaison de communication 3. Les deux terminaux reçoivent, par l'intermédiaire d'une antenne satellite 4, des données numériques diffusées par un opérateur de service, notamment des données audio/vidéo. Ils comportent chacun une carte à puce 15 / 25 dans laquelle sont stockés des droits de l'abonné pour accéder aux services de l'opérateur.

Les données reçues sont embrouillées, selon le principe classique de la télévision numérique payante, par des clés d'embrouillage (appelées souvent « Control Word ») et les clés sont elles-mêmes cryptées et transmises dans des messages notés ECM (acronyme de « Entitlement Control Message ») avec les données liées au service. Des messages personnalisés, notés EMM (de « Entitlement Management Message ») permettent de mettre à jour sur chaque carte à puces les « droits » dont dispose chaque abonné (ces droits pouvant également être reçus par une ligne téléphonique de l'abonné à laquelle est reliée le terminal, comme dans le cas du Pay per View par exemple). Pour désembrouiller un service auquel un abonné a droit, les ECMs sont envoyés à la carte à puce qui fournit les clés de désembrouillage décryptées correspondantes, ces clés permettant de désembrouiller le service. Les clés de désembrouillage sont dynamiques et changent au plus toutes les 10 secondes (« key period »).

Les données numériques embrouillées sont reçues par un tuner/démodulateur 10 / 20 dans chaque terminal 1 / 2. Un démultiplexeur et dispositif de filtrage 11 /21 extrait des données reçues les messages ECMs et EMMs qui sont dirigés vers un module de contrôle d'accès 14 / 24. Ce module 14 / 24 décrypte les clés de désembrouillage pour les transmettre à un désembrouilleur 12 / 22, lequel reçoit les données audio/vidéo A / V du module de démultiplexage et de filtrage 11 / 21. Grace aux clés de désembrouillage reçues du module 14 / 24, le désembrouilleur peut désembrouiller les données A/ V et les transmettre à un décodeur , notamment un décodeur MPEG 13 / 23 qui restitue en sortie des signaux audio / vidéo en clair pour un téléviseur.

Selon l'invention, un module de gestion de l'application d'appariement 17 / 27 est présent dans le terminal maître 1 et dans le terminal esclave 2. Il gère les communications entre les deux terminaux et en particulier le transfert des informations du terminal maître vers le terminal esclave pour permettre au terminal esclave d'accéder aux données reçues. Ce module contrôle également le délai qui s'écoule avant la réception de ces informations de manière à bloquer le fonctionnement du terminal esclave si les informations ne sont pas reçues dans le délai fixé. Un port de communication 16 / 26 disposé dans chaque terminal gère la liaison entre les deux terminaux.

La figure 2 illustre une première méthode d'implémentation de l'invention, basée sur les EMMs.

Elle consiste à fournir les droits (EMMs) du terminal numérique esclave par l'intermédiaire du terminal numérique maître et de la liaison de communication d'appariement, et non plus par l'antenne satellite. En pratique, le terminal numérique esclave 2 reçoit par satellite un EMM « EMM (Fin_de_droits) » qui efface tout ou partie des droits de sa carte à puce 25. Immédiatement après, il reçoit une information « Message (Demande_droits_au_Maître) » qu'il doit transmettre au terminal maître 1 par la liaison physique 3. Le terminal numérique maître utilise cette information pour capter un EMM émis peu de temps plus tard. Cet EMM « Message (Droits_esclave) » est ensuite immédiatement retransmis au terminal numérique esclave par la liaison de communication 3. Cet EMM « Message (Droits_esclave) » permet au terminal esclave 2 de mettre à jour ses droits dans sa carte à puce.

Si la réponse du terminal maître 1 n'est pas reçue dans un délai imparti (délai maximal Δt), le décodeur esclave se bloque, jusqu'à la prochaine émission d'EMMs.

On notera que la fréquence d'émission des EMMs peut être faible (un ou plusieurs jours). De plus, le délai maximal imparti Δt doit être suffisamment long pour que les terminaux numériques aient le temps de traiter les informations et suffisamment court pour qu'un retard introduit par un intermédiaire de type réseau Internet soit prohibitif et bloque le terminal esclave.

La figure 3 illustre une deuxième méthode d'implémentation de l'invention, également basée sur les EMMs.

Elle consiste à fournir au terminal numérique esclave 2 les informations de filtrage des EMMs par l'intermédiaire du terminal maître 1 et de la liaison de communication d'appariement 3.

Le terminal esclave reçoit un EMM « EMM (Suppression_de_droits) » qui annule tout ou partie des droits de sa carte 25. Immédiatement après, le terminal maître reçoit et retransmet cette fois un message contenant les paramètres de filtrage des EMMs « Message (Info de filtrage EMM Esclave) » du terminal esclave, ces informations devant être envoyées au terminal esclave par la liaison de communication 3 dans un temps donné.

Les droits sont ensuite diffusés par l'opérateur de services vers le terminal esclave 2 qui, grâce aux informations reçues du maître peut capter l'EMM contenant les droits de la carte « esclave » 25 et continuer de fonctionner normalement.

Si le terminal numérique esclave 2 n'a pas reçu à temps les informations de filtrage EMM, les droits ne sont pas restaurés, et le terminal esclave 2 ne fonctionne plus normalement.

D'autres variantes simples peuvent être envisagées : par exemple le terminal maître reçoit une partie de l'EMM (resp. ECM) du terminal esclave et la retransmet au terminal esclave dans un laps de temps limité.

Les implémentations décrites ci-dessus impliquent certaines contraintes d'utilisation du terminal maître : il doit être actif et en mesure de recevoir les EMMs/ECMs/messages en permanence, d'une part puisque la diffusion des informations par le système de diffusion n'est pas prédictible dans le temps et d'autre part parce que le système de diffusion n'a pas de retour d'information sur le fait que ces EMMs/ECMs/messages ont été reçus par leurs destinataires.

L'implémentation suivante illustrée par la figure 4 permet de réduire ces contraintes.

Selon ce mode de réalisation de l'invention, tout ou partie des droits du terminal esclave 2 sont reçus sous forme d'EMM et mémorisés par le terminal maître 1. Le terminal esclave 2 va demander au terminal maître une mise à jour de ses droits à un moment ultérieur.

Le moment où se fait l'échange d'informations peut être choisi de manière à garantir que cet échange sera un succès (par exemple juste après avoir vérifié que la communication entre les 2 décodeurs est opérationnelle et/ou s'être assuré de la présence de l'abonné près de son terminal esclave pour qu'il puisse suivre d'éventuelles instructions). L'opération doit cependant avoir lieu pendant un intervalle de temps limité (par exemple quelques jours) après l'arrivée des EMMs, sinon le module logiciel 27 du terminal esclave annule les droits de sa carte à puce 25.

Le moment approprié venu, le terminal esclave 2 demande l'information EMM au terminal maître 1, qui doit renvoyer cette information dans un délai maximum de quelques dizaines de millisecondes. Si l'information n'est pas reçue dans ce délai, le module logiciel 27 du terminal esclave annule les droits de sa carte à puce 25.

L'implémentation suivante qui est illustrée par la figure 5 permet de réduire un risque lié à l'émulation possible des messages envoyés par le terminal maître au terminal esclave par un dispositif extérieur.

Les informations qui sont fournies au terminal esclave sont extraites du flux diffusé par le système de diffusion par le terminal maître. Dans les deux premières implémentations, l'information reçue par le terminal maître 1 doit être transférée au terminal esclave 2 immédiatement après réception. Un dispositif pirate pourrait être tenté de retrouver une corrélation entre le message circulant sur la liaison de communication 3 et le contenu du flux transport diffusé reçu par le terminal maître dans les instants qui ont précédé, et ainsi être capable de reproduire le processus de traitement du flux transport pour générer un message identique pour le terminal esclave dans un délai suffisamment court. Ce dispositif pourrait être soit un ordinateur équipé d'un tuner / démodulateur / démultiplexeur, soit l'équivalent d'un autre décodeur avec un logiciel adapté, et être mis à proximité du terminal esclave, loin du terminal maître

Pour éviter qu'une telle corrélation puisse être trouvée, les informations reçues par le terminal numérique maître 1 doivent être transformées, selon cette implémentation préférée de l'invention, avant d'être

envoyées au terminal esclave 2. Le moyen le plus sûr disponible dans un terminal numérique pour effectuer cette transformation est l'utilisation du désembrouilleur DVB.

Dans la pratique, il s'agit donc d'envoyer au terminal maître 1 un ECM spécial, qui est transformé, dans la carte à puce maître15, en clé de désembrouillage. Le message contenant les informations pour le terminal esclave sont ensuite envoyées au terminal maître dans des paquets de données embrouillés avec cette même clé. Une fois désembrouillés, les paquets peuvent être traités par le terminal maître pour générer le message à destination du terminal esclave.

Cette méthode est applicable à toutes les variantes d'implémentation citées plus haut. Sur la figure 5, elle s'applique à la deuxième méthode d'implémentation de l'invention.

La figure 6 illustre quant à elle une autre variante d'implémentation permettant de résoudre un autre risque. Ce risque identifié en particulier pour le troisième type d'implémentation est celui de l'émulation par un dispositif externe des messages envoyés par le terminal esclave au terminal maître pour récupérer l'EMM stocké dans le terminal maître.

Un dispositif externe connecté au terminal maître pourrait ainsi émuler la demande du terminal esclave et intercepter la réponse du terminal maître. Cette réponse pourrait ensuite être envoyée par Internet à un autre dispositif externe relié au terminal esclave, qui pourrait alors fournir la bonne information lorsque le terminal esclave la demande.

Pour éviter une telle émulation, on peut proposer soit l'utilisation d'un protocole sécurisé avec authentification, soit plus simplement utiliser une fois de plus les ressources de la carte à puce et du système de diffusion.

Le système de diffusion peut en effet envoyer à un moment donné au terminal maître et au terminal esclave un un ECM spécial, qui est transformé, dans la carte à puce maître en clé de désembrouillage. Puis le système de diffusion envoie à chacun des terminaux un message identique (code secret), crypté avec ces clés préalablement reçues. Les messages contenant le code secret sont décryptés sur chaque décodeur par la carte à puce. Le terminal esclave 2 teste alors le code secret décrypté. Le terminal maître attend ce message pendant un laps de temps limité. S'il le reçoit à temps, il vérifie qu'il s'agit bien du code secret attendu en le comparant à celui qu'il a lui-même reçu, puis répond en envoyant l'EMM au terminal esclave. S'il n'a pas reçu le message attendu dans les temps, il n'envoie pas l'information

EMM. Une fois son message envoyé, le terminal esclave attend lui aussi la réponse du maître pendant un laps de temps limité. Si l'information EMM n'arrive pas dans les délais impartis, le terminal esclave ne remet pas les droits de sa carte à puce à jour.

Un tel dispositif permet donc, d'une part de rendre non-prédictible l'échange d'informations, et d'autre part impose la contrainte de temps réel qui évite un contournement potentiel par Internet.

REVENDICATIONS

1. Système de réception de données numériques diffusées comprenant

un terminal numérique maître ( ), et

au moins un terminal numérique esclave ( ) raccordé au terminal maître par une liaison () et susceptible de recevoir des données numériques protégées,

caractérisé en ce que ledit terminal numérique esclave ne peut accéder auxdites données protégées que si des informations nécessaires pour accéder auxdites données et reçues par le terminal numérique maître sont transmises par l'intermédiaire de ladite liaison ( ) au terminal numérique esclave dans un délai prédéterminé.

2. Système selon la revendication 1, caractérisé en ce que lesdites informations reçues par le terminal numérique maître sont transformées avant d'être transmises au terminal numérique esclave.

3.

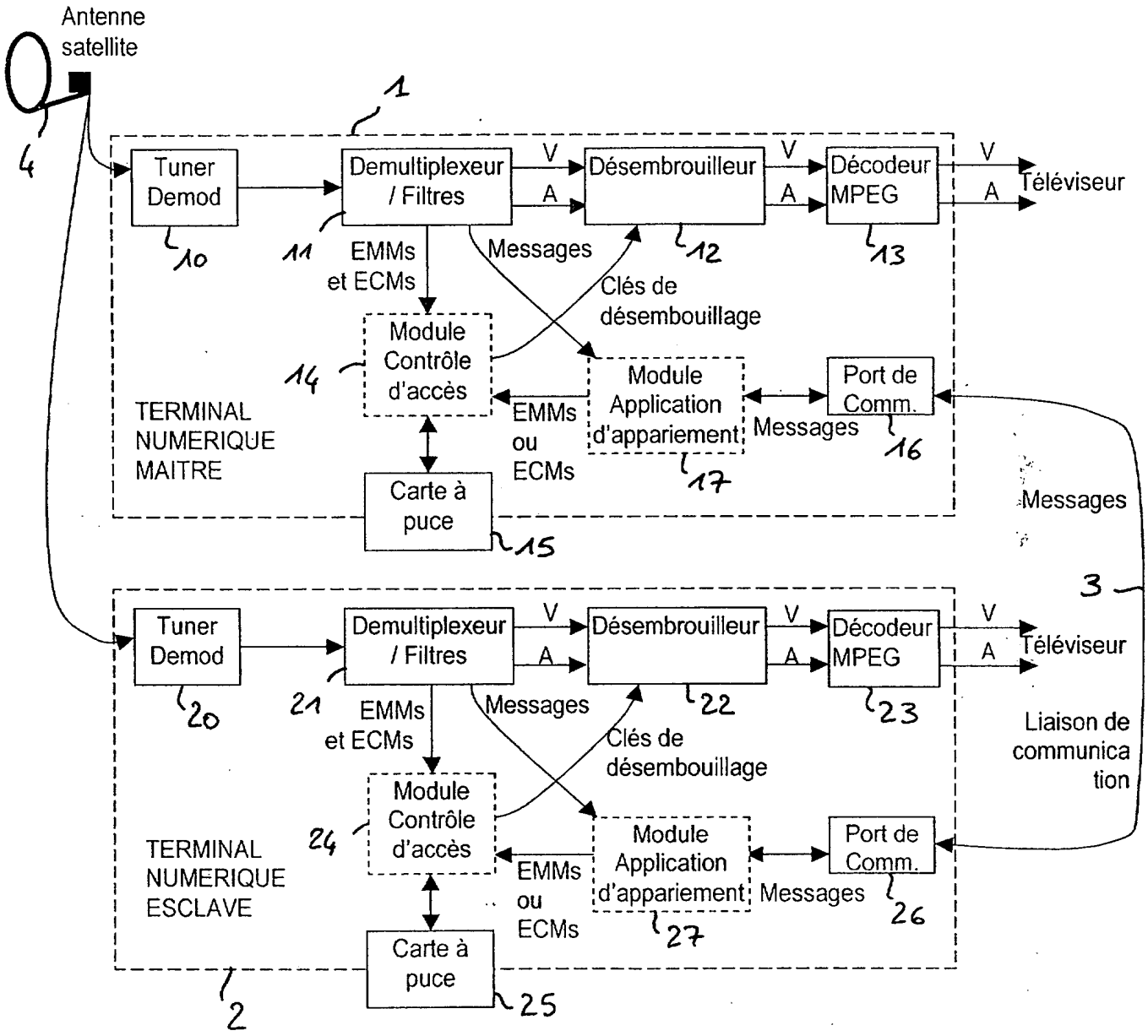

Antenne satellite
4
1
Tuner Demod
10
Demultiplexeur / Filtres
11
V
A
Désembrouilleur
12
Décodeur MPEG
13
Téléviseur
EMMs et ECMs
Messages
Clés de désembouillage
Module Contrôle d'accès
14
Module Application d'appariement
17
Port de Comm.
16
TERMINAL NUMERIQUE MAITRE
EMMs ou ECMs
Carte à puce
15
Messages
3
Tuner Demod
20
Demultiplexeur / Filtres
21
Désembrouilleur
22
Décodeur MPEG
23
Téléviseur
Liaison de communication
EMMs et ECMs
Messages
Clés de désembouillage
Module Contrôle d'accès
24
Module Application d'appariement
27
Port de Comm.
26
TERMINAL NUMERIQUE ESCLAVE
EMMs ou ECMs
Carte à puce
25
2

Fig. 1

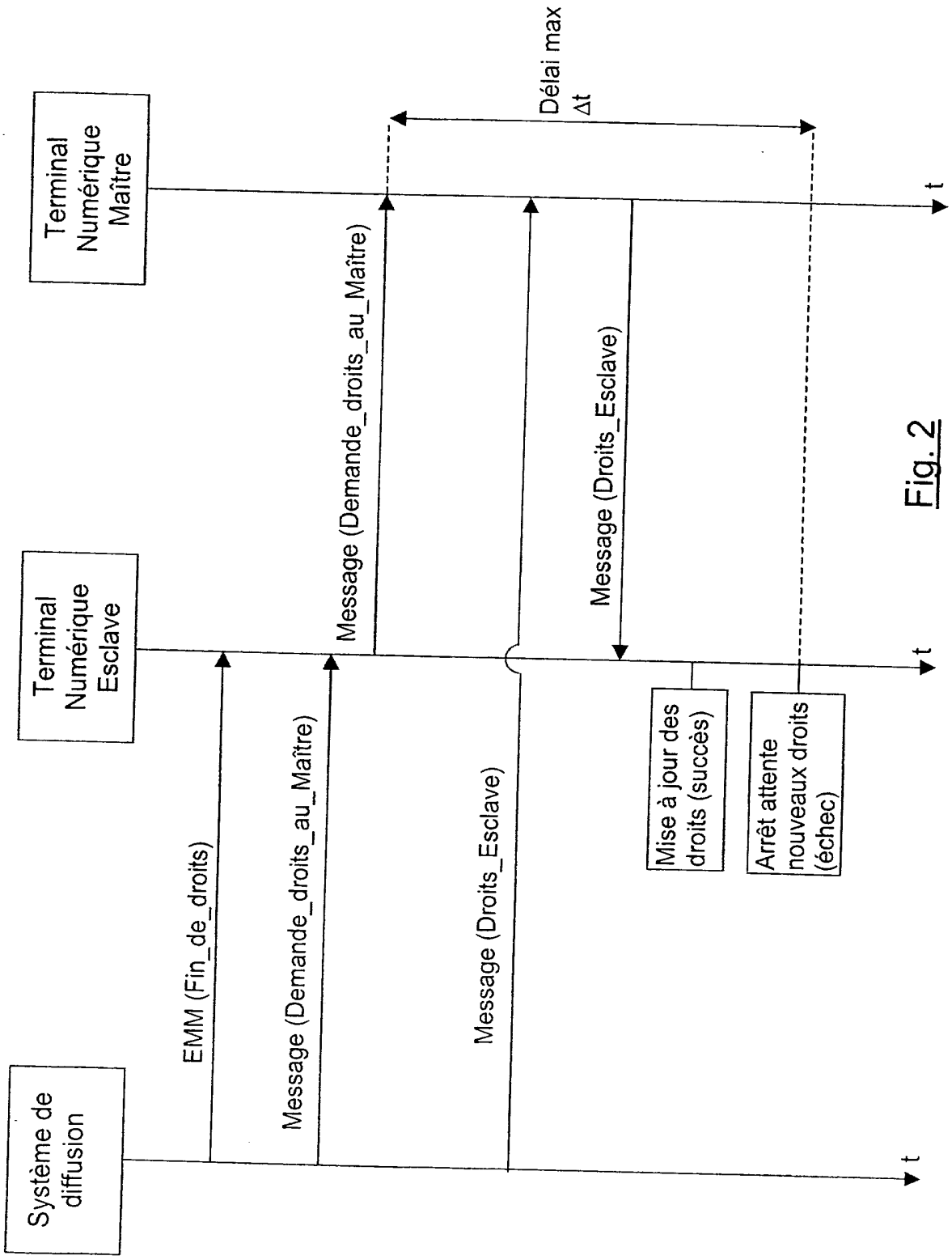

Terminal Numérique Maître
Délai max
Δt
t
Message (Demande_droits_au_Maître)
Message (Droits_Esclave)
Terminal Numérique Esclave
t
Mise à jour des droits (succès)
Arrêt attente nouveaux droits (échec)
EMM (Fin_de_droits)
Message (Demande_droits_au_Maître)
Message (Droits_Esclave)
Système de diffusion
t

Fig. 2

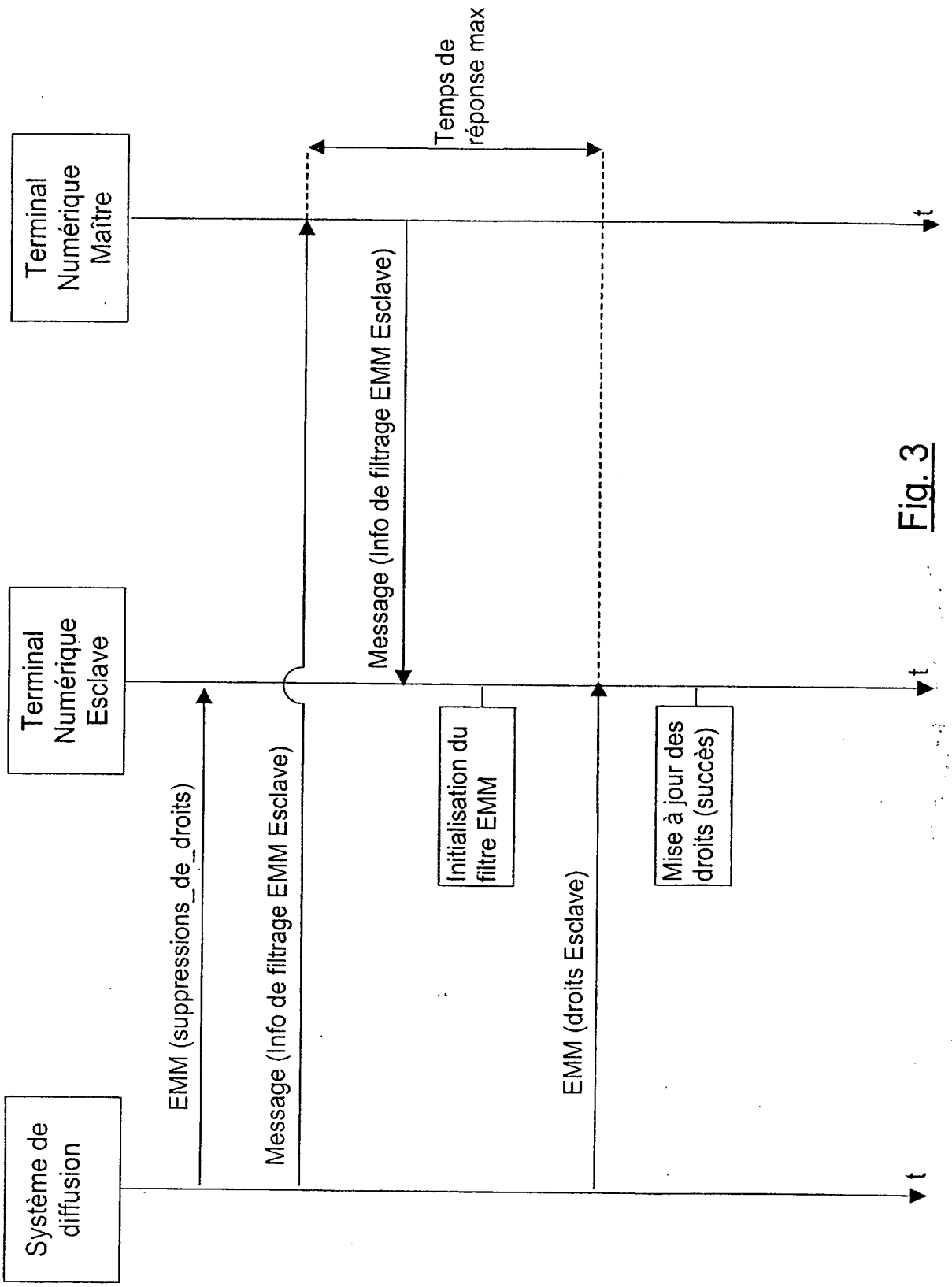

Terminal Numérique Maître
Terminal Numérique Esclave
Système de diffusion
Temps de réponse max
Message (Info de filtrage EMM Esclave)
EMM (suppressions_de_droits)
Message (Info de filtrage EMM Esclave)
Initialisation du filtre EMM
EMM (droits Esclave)
Mise à jour des droits (succès)
t
t
t

Fig. 3

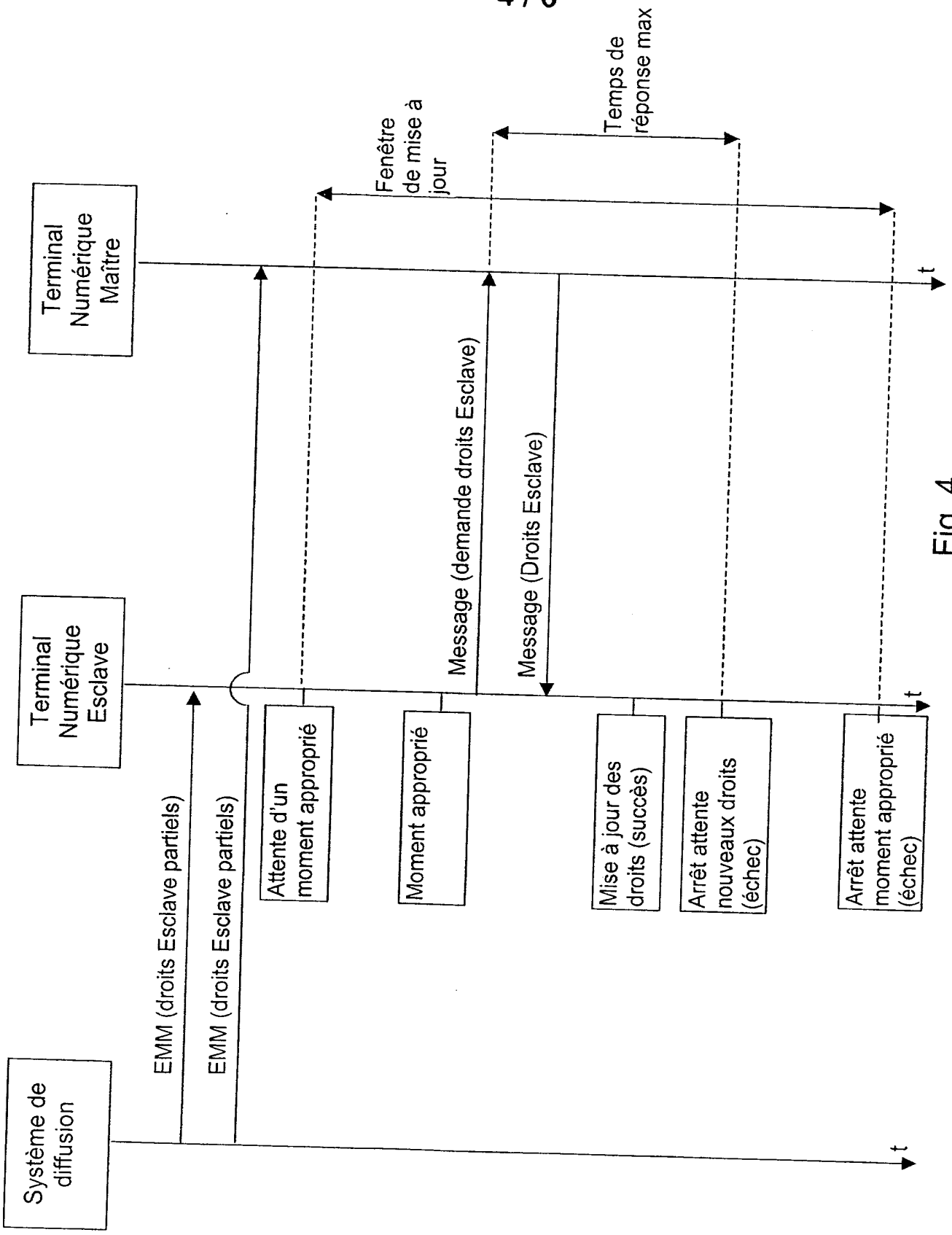

Terminal Numérique Maître
Terminal Numérique Esclave
Système de diffusion
Fenêtre de mise à jour
Temps de réponse max
EMM (droits Esclave partiels)
EMM (droits Esclave partiels)
Attente d'un moment approprié
Moment approprié
Message (demande droits Esclave)
Message (Droits Esclave)
Mise à jour des droits (succès)
Arrêt attente nouveaux droits (échec)
Arrêt attente moment approprié (échec)
t
t
t

Fig. 4

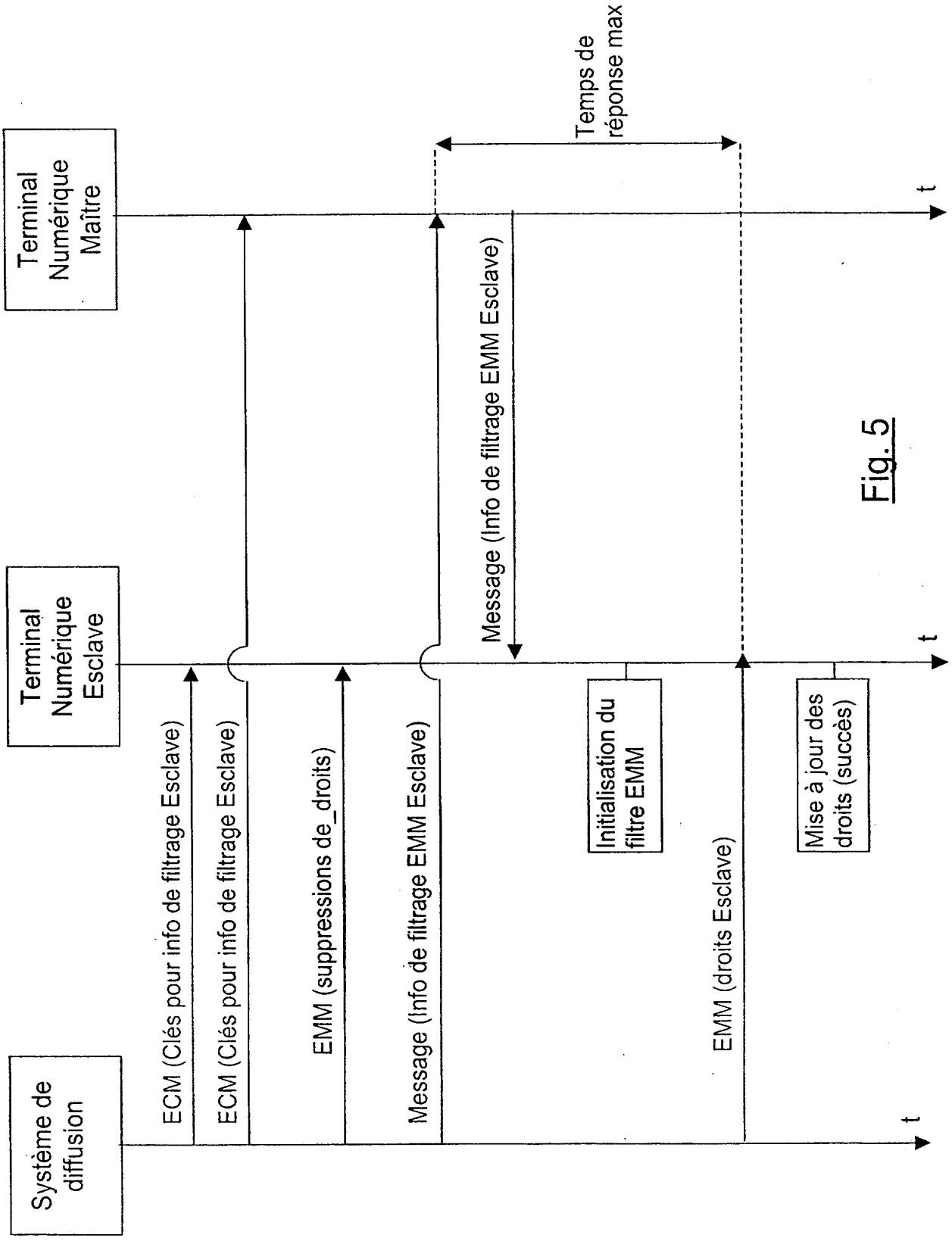

Terminal Numérique Maître
Terminal Numérique Esclave
Système de diffusion
Temps de réponse max
t
t
t
Message (Info de filtrage EMM Esclave)
ECM (Clés pour info de filtrage Esclave)
ECM (Clés pour info de filtrage Esclave)
EMM (suppressions de_droits)
Message (Info de filtrage EMM Esclave)
Initialisation du filtre EMM
EMM (droits Esclave)
Mise à jour des droits (succès)

Fig. 5

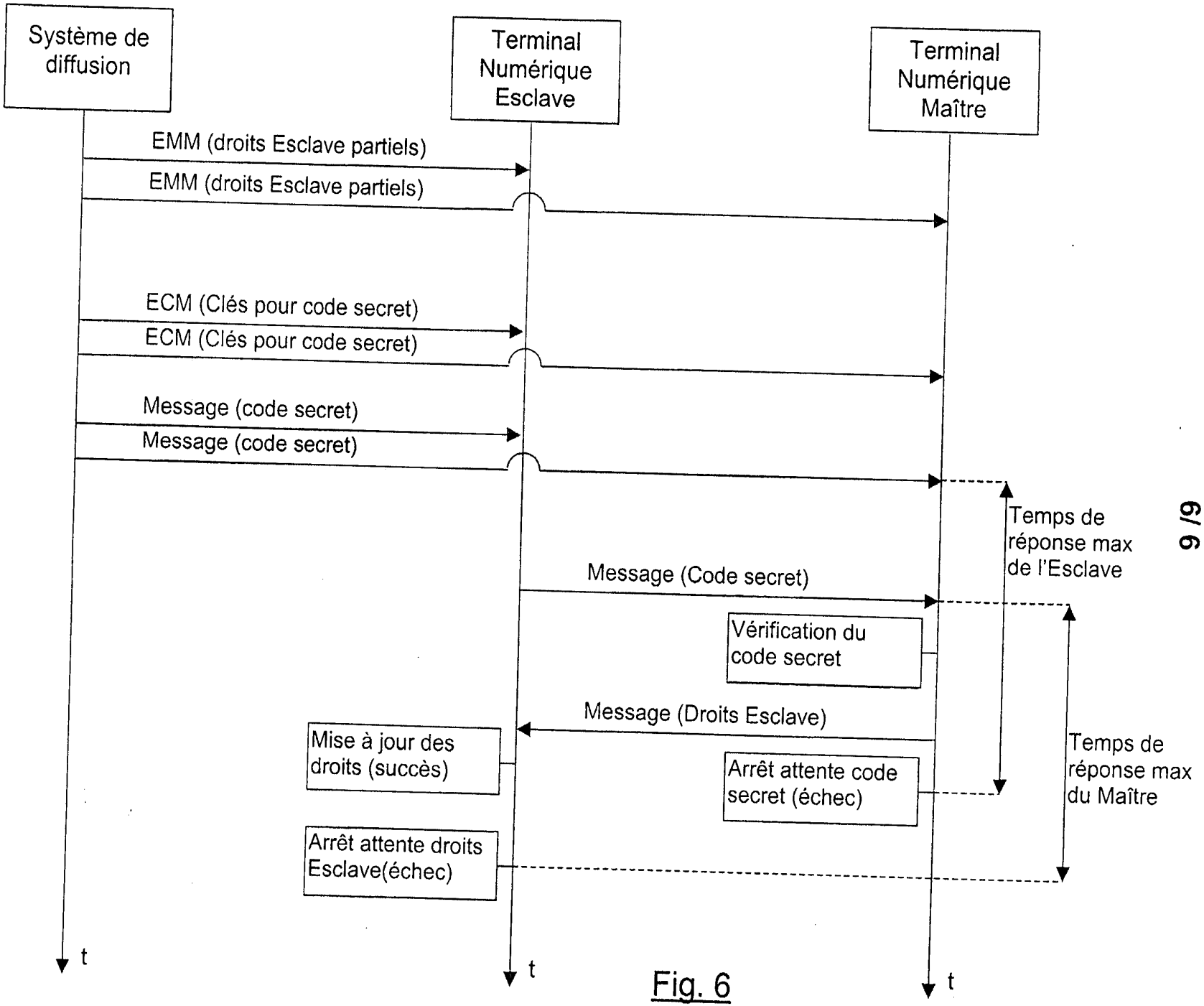


Fig. 6

reçue le 31/03/03

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

INV

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier *(facultatif)*	PF030028
N° D'ENREGISTREMENT NATIONAL	0300941

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Système de réception de données numériques diffusées comprenant un terminal numérique maître, et au moins un terminal numérique esclave

LE(S) DEMANDEUR(S) :

THOMSON LICENSING S.A
46 Quai Alphonse Le Gallo
92100 Boulogne Billancourt
FRANCE

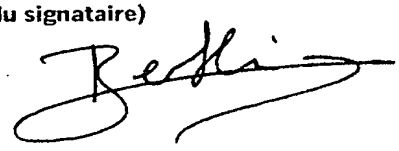
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		LEYENDECKER
Prénoms		Philippe
Adresse	Rue	10 rue Paul Duplessis
	Code postal et ville	37410 Chateaugiron
Société d'appartenance *(facultatif)*		
2 Nom		CUEFF
Prénoms		Jean-Maurice
Adresse	Rue	23 rue Mordillat
	Code postal et ville	92260 Fontenay aux Roses
Société d'appartenance *(facultatif)*		
3 Nom		CREUSOT
Prénoms		Daniel
Adresse	Rue	4 rue des Tulipes
	Code postal et ville	78960 Voisins le Bretonneux
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Karine BERTHIER
Mandataire



La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.